Declassified and Approved For Release 2012/02/06 : CIA-RDP91-00561R000100010003-7

APPEARED
ON PAGE A1

WASHINGTON POST
13 November 1986

U.S. Limits Access to Information Related to National Security

By Michael Schrage
Washington Post Staff Writer

National security adviser John Poindexter last week signed a memorandum that gives federal departments broad new powers to limit release of government data and creates a new "sensitive" classification to restrict access to national security related information.

The memorandum, signed Nov. 6, is part of the Reagan administration's continuing efforts to create mechanisms, such as stringent export controls, to deny certain kinds of technical and economic information to the Soviet bloc.

The new measures are being carried out under National Security Decision Directive 145 of September 1984, a presidential order that created a top-level interdepartmental group to explore ways, ranging from telephone scrambling to data encryption systems, to better protect government information.

The government has also been worried that foreign powers could acquire valuable information by tapping into both private and government computerized data bases that allow public access. Operators of such data bases have been interviewed in recent months by government officials about the practicality of denying access to anyone who might represent a foreign power.

However, Donald C. Latham, assistant secretary of defense for communications, command, control and intelligence, and chairman of the interdepartmental group, said that the "sensitive" classification is meant to deal with that problem by preventing the information from getting onto the data bases in the first place.

According to Latham, Poindexter had to approve the definition before it went into effect.

"This was very carefully thought through with the lawyers and everybody," Latham said.

Latham declined to call the "sensitive" category a new level of classification, instead describing it as an "information protection mechanism."

The memorandum offers "guidelines to be considered, not an edict that must be followed," said Latham, who added that it "should not inhibit" requests made under the Freedom of Information Act.

However, the memorandum grants to the heads of federal agencies authority to apply the new "sensitive" label as they choose. Information so designated could not be disseminated outside the government. This authority would resemble the powers that the departments of state and defense now have to classify data and documents, but would not require extensive physical security measures that now must be used with classified material.

The memorandum also leaves numerous details to be worked out.

For instance, Latham indicated that individuals in unauthorized possession of "sensitive" national security related materials might be subject to penalties. However, he would not specify what these might be. Similarly, it is unclear whether federal employes who disclose "sensitive" material will be liable to penalties, disciplinary action or dismissal.

The memorandum describes "sensitive" national security material as "those unclassified matters that are related to the national defense or foreign relations of the U.S. government," including "a wide range of government or government derived" arenas from economics to technology to industry to finance to agriculture.

"The federal government will pursue very heavily information protection both for unclassified sensitive and unclassified sensitive national security related information," said Diane Fountain, the director of the information systems directorate in Latham's office, in a session Tuesday night at the Information Industry Association conference in New York.

Fountain underlined the national security community's concern that individuals with personal computers here or overseas could easily access sensitive material on computer data bases such as Mead's Nexis and Dialog.

The Air Force has recently completed a classified report on the topic of data bases that explores such recommendations as requiring licenses for foreigners who want to access U.S. data bases and the use of special software that monitors national security-related topics in data bases, Fountain noted. The government is also exploring steps to curtail access to the defense related information in the government's National Technical Information Service and the Defense Technical Information Center.

"There is a very basic need for government and industry cooperation in this area," she said. "I don't believe the issue is whether or not we're going to protect—the issue is what we're going to protect and how."

However, Latham said that by the time sensitive information gets into a commercial data base, it's too late to protect it. Consequently, he sees the new "sensitive" classification as a means to stop the flow of certain kinds of data into the public domain.

"If it's sensitive, it shouldn't go in there," said Latham. "But we're not going to be a policeman."

Still, defense deputy undersecretary for trade security policy Stephen Bryen observes that the new "sensitive" classification should make it easier to stop the export of technical information that could be used by the Eastern bloc for military purposes.

Larry Simon, professor of constitutional law at the University of Southern California, said the government is probably within its constitutional authority in applying such restrictions.

"The way the court has shaped this area of the law is that the government does have constitutional powers—very substantial power—to stop employes from giving out information," he said.

However, he added, that "whenever the government allows its own agencies [other than those concerned with defense] to keep secret information, that's very significant."

Declassified and Approved For Release 2012/02/06 : CIA-RDP91-00561R000100010003-7